The Economic Design of Consensus Incentive Methods

Iarla Molloy

Abstract: Incentives play a key role in the success and sustainability of blockchain solutions. Their effect and impact range the whole spectrum from miner rewards, staking rewards, transactions-fee and play a role in the critical design of the blockchain. In this paper, we explore the economic impacts of consensus design decisions and design a framework to capture the economic consequences of specific incentive intents. A consensus method e.g. (Proof of Work, Proof of Stake) is the mechanism use by distributed systems achieve an agreement on state of the blockchain in turn maintaining the blockchain integrity. Each of these mechanisms are designed to reward actors; a summary of the mechanisms is explored in this paper with their design goals.

Keywords: Blockchain, Incentives, Economics, Consensus, PoW, PoS

1. Introduction

Incentives are the pillar of successful permissionless blockchains. We explore the economic objectives behind the Proof of Work (PoW) and Proof of Stake (PoS) consensus designs. We introduce a simplified model called Blockchain Incentive Rewards (BIR) to capture the scope of the different consensus types.

2. Literature Review

This section provides a review of existing literature in the areas of the blockchain incentive schemes, PoW and PoS systems. It finishes up with a brief look at the verifiers dilemma.

2.1. Survey of blockchain incentive schemes

Catalini and Gans (2020) point to incentives being created through organic growth of blockchain where early adopters benefit from early engagement. They categorize incentives into two classes; adoption phase and incentives phase to support continuous contribution. The first phase can include the issuing of the tokens through an Initial Coin Offering (ICO) scheme, while the second phase incentives are created through consensus mechanisms. Groups incentive strategies into two primary groups; issuing a token in response to what a network node deserves and based on the allocation of the tokens (Huang et al. 2019). In the issuing mechanism for example Bitcoin, nodes win invoicing rights under PoW consensus algorithms and Bitcoin rewards the miners. The second method manages the distribution of existing tokens in the system through evaluating the nodes contributing to the network, the contribution of each node and the random factors that guarantee fairness. In the original allocation model proposed by Nakamoto (2008), the first miner that succeeds can get a bitcoin while the rest all fail and can only expect the next turn although they paid the computing power to go through mining pools.

2.2. Incentives and Proof of Work systems

In a PoW consensus, solution miners have separate functions; creating blockchains and checking the validity of each blocks. Luu et al. (2015) discuss the concept of verifiers dilemma (resulting as consequence of lack of incentives in the PoW protocol). The miners get paid for the work done and use the rewards system as financial incentives. In the original bitcoin paper by Nakamoto (2008), the first transaction in a block starts a new coin. Blocks can only be added by

solving a complex hash function. The hashing power for the PoW system can be provided by individual miners or mining pools. The mining pool combine resources and shared rewards using schemes such as Pay-Per-Share (PPS) and Full Pay-Per-Share amongst others (Bitcoin, 2020).

2.3. Incentives and mining pools

Wang et al. (2020) point out several limitations associated within the mining pools that can influence the motivational effects of mining pool. One of these limitations is the security of the hardware and selection of mining pools (in 2018 – the top 5 mining pools had over 60% of the hashing power). They also outline dishonest actor strategies such as self-mining attacks (an attack where a miner does not release a block and creates a private fork) which can bias a mining pool. The existence of mining pools shifts the blockchain principle from a decentralized metaphor towards semi-centralized command and control metaphor. There are many reward types associated with each of the mining pools (Bitcoin, 2020).

2.4. Incentives and governance

Blockchain governance is explored by Beck et al. (2018) under three dimensions; decision rights, accountability and incentives. They point out that there are several target areas for the incentives such as incentives for users, systems development, token holders and technical consensus. In platforms such as Polkadot, they have inbuilt governance mechanism e.g. 'Dot' holders can create governance proposals and voting rights as shown in Figure 1 (Petrowski, 2020).

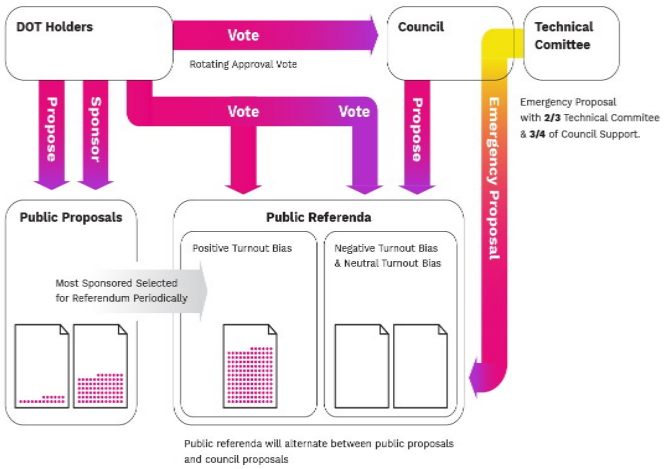


Figure 1. Polkadot Governance. Petrowski (2020).

The governance on a blockchain impacts the reputation of the blockchain and how the market behaves on the blockchain.

2.5. Reputation based incentives

In Wang et al. (2020), a reputation-based incentive scheme is proposed in the consensus process. Reputation networks have their origins in the early P2P networks, but a model proposed by the Gupta at al. (2003) model trust and reputation in decentralized multi-agent systems. Their model is built off the Entropy model which captures the exchange of the trust in the business environment. The Proof-of-Reputation is a proposed mechanism that can be integrated into the consensus protocols. They propose a new set of rules in the mining process in that it is the reputation decline if nodes fail to produce blocks within a period.

2.6. Incentives and Proof of Stake systems

PoS addresses issues with PoW systems by providing a consensus mechanism that is not impacted by computation cost and consensus time delays. The main idea of a PoS consensus mechanism is that the proportion of users' stake in the system is inversely proportional to the difficulty of block generation. The larger the stake held by nodes in the system, the easier the holder windows wins. In a preliminary paper by Fanti at al. (2019), economic rewards in PoS systems can be manifested in two ways; block rewards which are given to the proposer of the longest chain and transaction fees paid by the sender for transferring the amount which is split between a set of validators and the block proposer.

2.7. Incentives blockchain architectural layer

Huang et al. (2018) have categorized incentives into two primary areas; issuance and allocation. Issuance, which is typically associated with the public blockchain provides rewards to miners who contribute resources such as CPU/network or storage to the upkeep of the network. The allocation incentives are designed to ensure that there are incentives for the continuous processing and forwarding of data on the network. Li et al. (2020) divide the architecture into multiple layers as shown in Figure 2 below. The combination of the incentive and consensus layers are a key fabric of the blockchain. In the architecture, the incentive layer plays a key role in the blockchain solutions. We extend this work by making the incentive layer orthogonal to all the other architecture layer and we include a new governance layer.

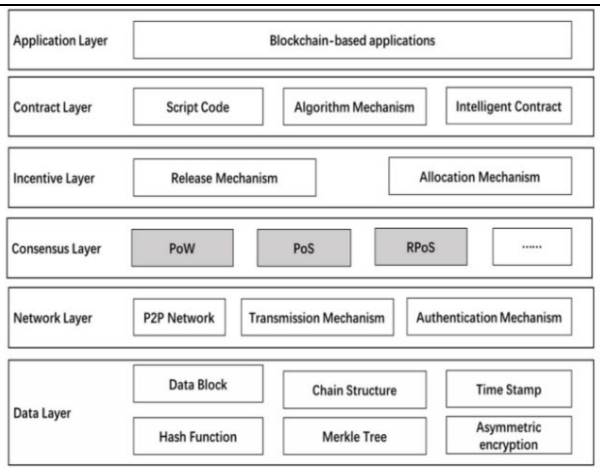


Figure 2. Blockchain layers. Li et al. (2020).

2.8. & Incentive compatibility

Luu et al. (2015) describes the verifiers dilemma as a situation in which rational miners are incentivized to accept invalid blockchains or decide to skip the verification of expensive transactions. They cite two potential attack resource exhaustions (using the Ethereum gas to include resource-intensive transaction in new blocks) or incorrect transaction attacks (skipping part of the attacks that are compute intensive). Incentive compatibility occurs when the incentives that motivate the actions of individual participants are consistent with following the guidelines established by the group for the common good. Chiu and Koeppl (2019) describe modelling incentives as the No-Double-Spending constraint (NoDS) which outlines how reward and confirmation lags play a critical role in the design incentives to prevent users from double sending.

3. PoW Economics and Incentives

PoW miners have separate functions in consensus; checking that it is that blocks are correctly constructed and checking the validity of each blocks. The contribution of the work by Luu et al. (2015) includes the introduction of the verifier's dilemma. The miners get paid for the work done and use the rewards system as financial incentives. The work originates in the original bitcoin implementation.

3.1. Individual miner economics

Individual miner can earn revenue from the mining the blockchain but need to buy hardware and pay energy costs. Once a complex puzzle is solved and a block

is created, the miners are given rewards. A lot of energy is expended when solving the puzzle which make the expense quiet intimidating thus the need for pools.

3.2. Mining pool monopolies

In a study by Silva et al. (2020) on the Ethereum network, they identified selfish behavior within the pools and the prevalence that these power mining pools have impacted the blocked delays. Their analysis looked at fifteen mining pools that created most of the blocks, with Sparkpool and F2Pool2 holding approximately 61% of the hash power. A study by Miller et al. (2015) concluded that 2% of nodes accounted for 75% of mining power. These monopolies can act as a disincentive for new miners to engage in the consensus.

3.3. ASIC economics and mining pools

In order to mine a cryptocurrency, a miner will need an upfront investment in the ASICs. The cost prices that are based ASIC hardware is typically based on the expected returns from the hardware. Yaish and Zohar (2020) argue the contrary by showing that the underlying hardware can be considered as financial options. Their analysis also showed that a reduction in Bitcoin volatility negatively impacts the value of the hardware and thus becomes a financial disincentive. The energy cost of running the equipment is important from an individual's mining/pooling perspective. Initial estimates from De Vries (2020) calculated that in 2018, the total consumption of the bitcoin network equalled the consumption of energy in Ireland.

4. PoS Economics and Incentives

PoS protocols were developed as energy saving alternatives to PoW. Instead of computational power resources, leaders are selected based on their stakes, i.e., contributions to the blockchain network.

The algorithms use a Follow-the-Satoshi (FTS) algorithm that have been adopted in PoS based blockchain networks such as Cardano, Sp8de, and Tezos. The staking rewards are created through inflation and the reward scheme is designed to incentive consensus participation by rewarding block creators and validators while at the same time penalizing poor behaviors' and prevent attacks. Table 1 below shows these consensus protocols

Table 1. Consensus Protocols

Protocol	Incentive scheme
Casper	Deposit confiscated for poor validator - behaviors
Algorand	Pure POS (every node can particulate in the network)
Tendermint	Rewards divided between validators and deposit confiscated for mis-behaviors

4.1. Ethereum transition to POS

Ethereum (2020) is transitioning away from a PoW system towards a PoS system in which validators will be paid to perform tasks to ensure the network is healthy. The incentive stakes influence the number of validators on the network and cost of the network. There are several factors that a validator must consider before taking up an incentive; computing costs, capital acquisition cost (deposit of 32 ETH), cost risk and general uptime of a maintenance cost and security risk. Polkadot is a multi-chain network that connects blockchain and uses a NPoS protocol as its consensus mechanism in which it nominates a subset of validators that can perform the consensus. There is a limited number of validators that get equal powers and equal rewards.

4.2 DeFi as a dis-incentive for PoS

Incentives from the PoS have competition from new offerings in the DeFi space. The PoS requires validators to commit their assets to earn rewards while decentralized financial application such as Compound and maker provide ways in which the user and validators can lock-up Ethereum from the blockchain. The white papers on the asset protocol from Park et al. (2020) outlines these problems in detail:

- Staking can damage the ecosystem as the new DeFi lending offers higher rates.
- Tokens that are DeFi staked cannot contribute to network security.
- Staked tokens cannot be traded as their true value cannot be reflected on the market.

4.2.1 Voting mechanism for disincentives

The nature of staking can lend itself to monopolies. EOS is a blockchain similar to Ethereum but in EOS there is an option to buy votes which slew the democracy of the blockchain producers. EOS however only runs 21

miners. Significant development has occurred in the PoS consensus mechanism over the last few years.

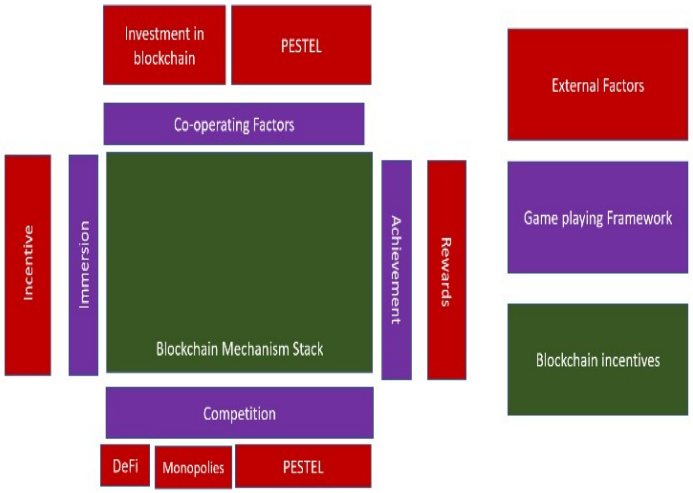
5. Design of the Model

In this section we will test the consensus models against a reference model that captures the economics decisions that influence the design mechanism used in the blockchain. We refer to this as the Blockchain Incentive Reward (BIR) model.

5.1 BIR Model

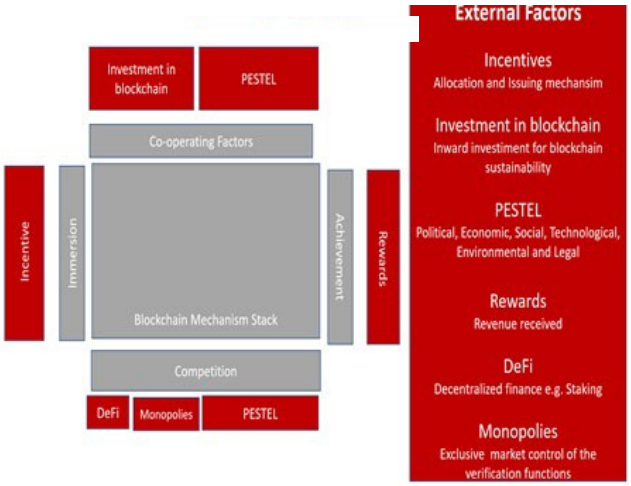
The model is captured below in Figure 3. The model is derived from Rakoff's Gameplay Model game playing model is assessed on co-operating, competition, immersion and achievement Albertarelli et al. (2018). The framework is composed of three tiers; external factors, game playing framework and blockchain mechansim stacks. These are decribed below in Figure 3.

Figure 3. BIR Model. Albertarelli et al. (2018)



5.1.1 External Factors

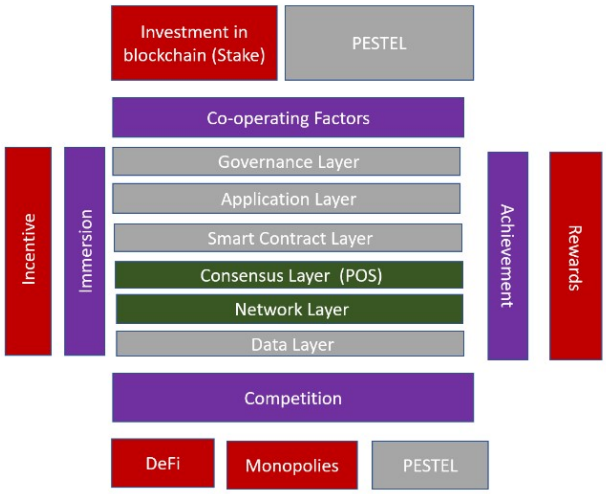
This tier captures the external factors such as PESTEL and the rewards and state of the dependent markets that might influence an agent's decision to engage in the consensus mechanism.



The PESTEL factors can be a co-operating (political beliefs) and a competitive factor to the blockchain e.g. cost of energy. The incentives can be allocations or issuance orientated.

5.1.2 Game Playing Framework

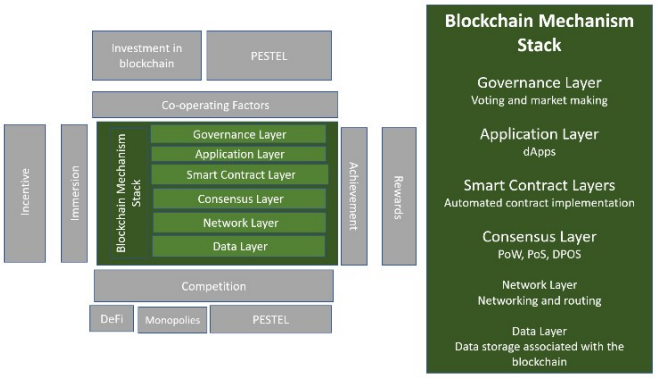
This tier will capture the agents state and motivations to engage in blockchain incentives. These states can be co-operating, competition and achievement orientated of immersive factors.
Defi monopolies are competitive factors to incentives while staking is seen as positive incentive factor.
Figure 5. Game Playing Framework. Albertarelli et al. (2018)



. Albertarelli et al.

5.1.3 Blockchain Mechanism Stack

In this tier the incentives can be applied several levels within the blockchain. The incentives can be applied at multiple technical layers within the technology stacks. Sometimes an incentive might span multiple layers in a stack.



5.2 Testing the model

This section outlines how each consensus can be mapped into the framework.

5.2.1 Analyzing Proof of work

The are some notes from this model, in order to co-operate into the network you need to invest while energy costs and mining pools could be a competition factor.

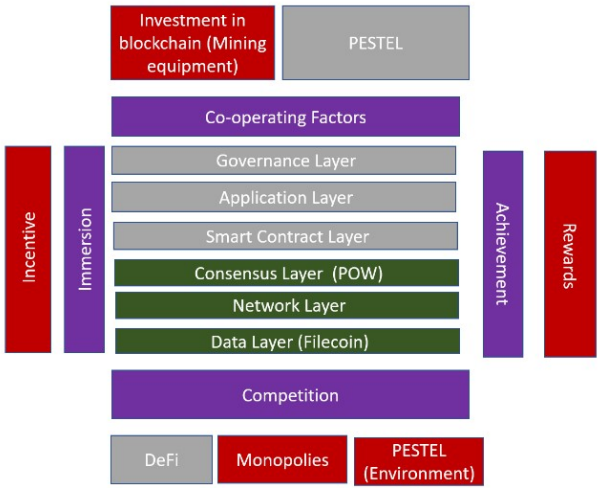
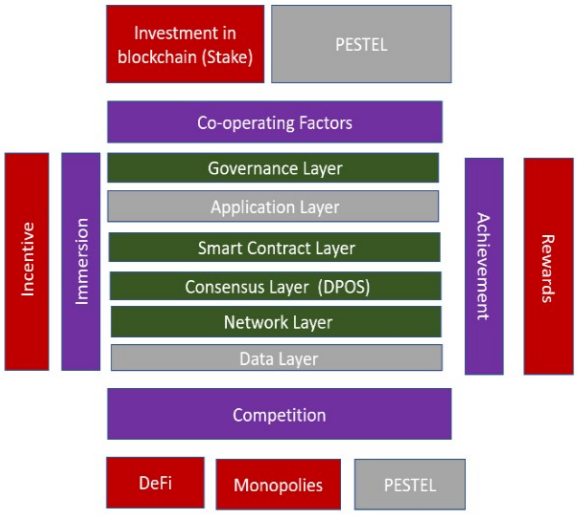


Figure 5. PoW consensus. Albertarelli et al. (2018).

5.2.3 Analyzing Proof of Stake

The investment is the PoS stake while the competition factor is DeFi.

If we look at the nPOS model the governance layer is activated.



6. Conclusions and future directions

We captured academic research into incentives behind the consensus mechanism. As part of the exploration there are number of key observations:

- The PoW mechanisms will be superseded by more advanced forms of PoS.
- The DeFi investment options can have a negative impact on the returns PoS systems.
- The governance and voting the model when considering investing option.
- The Data/Network layer outline in the document can be converged into a verifier layer.
- The BIR external model needs to be refined and the layers coding to create a simulation tools for incentives

—

References

Albertarelli, S., Fraternali, P., Herrera, S., Melenhorst, M., Novak, J., Pasini, C., Rizzoli, A. and Rottondi, C., 2018. A Survey on the Design of Gamified Systems for Energy and Water Sustainability. *Games*, 9(3), p.38.

Beck, R., Müller-Bloch, C. and King, J., 2018. Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for Information Systems*, pp.1020-1034.

Bitcoin. 2020. Comparison of mining pools. [online] Available at: https://en.bitcoin.it/wiki/Comparison_of_mining_pools. [Accessed 5 November 2020].

Catalini, C., Gans, J., 2020. Some simple economics of the blockchain. *Communications of the ACM*, 63(7), pp.80-90.

Chiu, J. and Koeppl, T., 2019. Incentive Compatibility on the Blockchain. *Studies in Economic Design*, pp.323-335.

Ethereum. 2020. Eth 2.0 Economics. [online] Available at: https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/eth-2.0-economics/. [Accessed 9 November 2020].

Fanti G, Leonid Kogan L., Viswanath P. 2019 Economics of Proof-of-Stake Payment Systems.

Gupta M., Judge P., Ammar M. (2003), A reputation system for peer-to-peer networks, Proceedings of the 13th International Workshop on Network and Operating Systems Support for Digital Audio and Video, ACM (2003), pp. 144-152

Huang, J., Lei, K., Du, M., Zhao, H., Liu, H., Liu, J. and Qi, Z., 2019. Survey on Blockchain Incentive Mechanism. *Communications in Computer and Information Science*, pp.386-395.

Li, A., Wei, X. and He, Z., 2020. Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. *Sustainability*, 12(7), p.2824.

Luu, L., Teutsch, J., Kulkarni, R. and Saxena, P., 2015. Demystifying Incentives in the Consensus Computer. *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp.706-719.

Miller A., Litton J., Pachulski A., Gupta N., Levin D., Spring N. and Bhattacharjee B., 2015. Discovering bitcoins public topology and influential nodes.

Nakamoto, S., 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. SSRN Electronic Journal.

Li, A., Wei, X. and He, Z., 2020. Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems. *Sustainability*, 12(7), p.2824.

Park R., Kim J., Hong D. (2020) https://anchorprotocol.com/docs/The_bAsset_Protocol.pdf. [online]. Available at: https://anchorprotocol.com/docs/The_bAsset_Protocol.pdf [Accessed 12 April 2020].

Petrowski, J., 2020. Polkadot Governance. [online]. Available at: https://polkadot.network/polkadot-governance/ [Accessed 2 April 2020].

Silva, P., Vavřička D., Barreto J. and Matos M., 2020. Impact of Geo-Distribution and Mining Pools on Blockchains: A Study of Ethereum - Practical Experience Report and Ongoing PhD Work. *2020 50th Annual IEEE-IFIP International Conference on Dependable Systems and Networks-Supplemental Volume (DSN-S)*.

de Vries, A., 2020. Bitcoin's energy consumption is underestimated: A market dynamics approach. *Energy Research & Social Science*, 70, p.101721.

Wang, E., Liang, Z., Chen, C., Kumari, S. and Khan, M., 2020. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Future Generation Computer Systems*, 102, pp.140-151.

Yaish, Aviv & Zohar, Aviv., 2020. Pricing ASICs for Cryptocurrency Mining